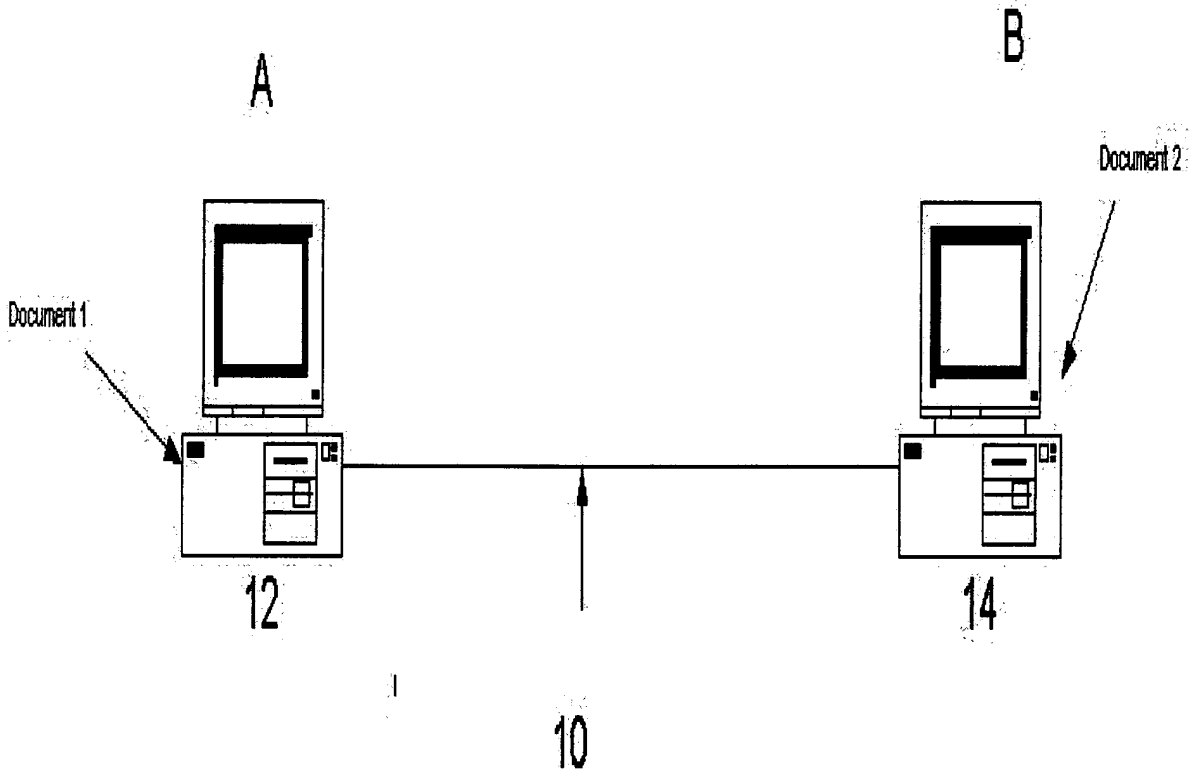
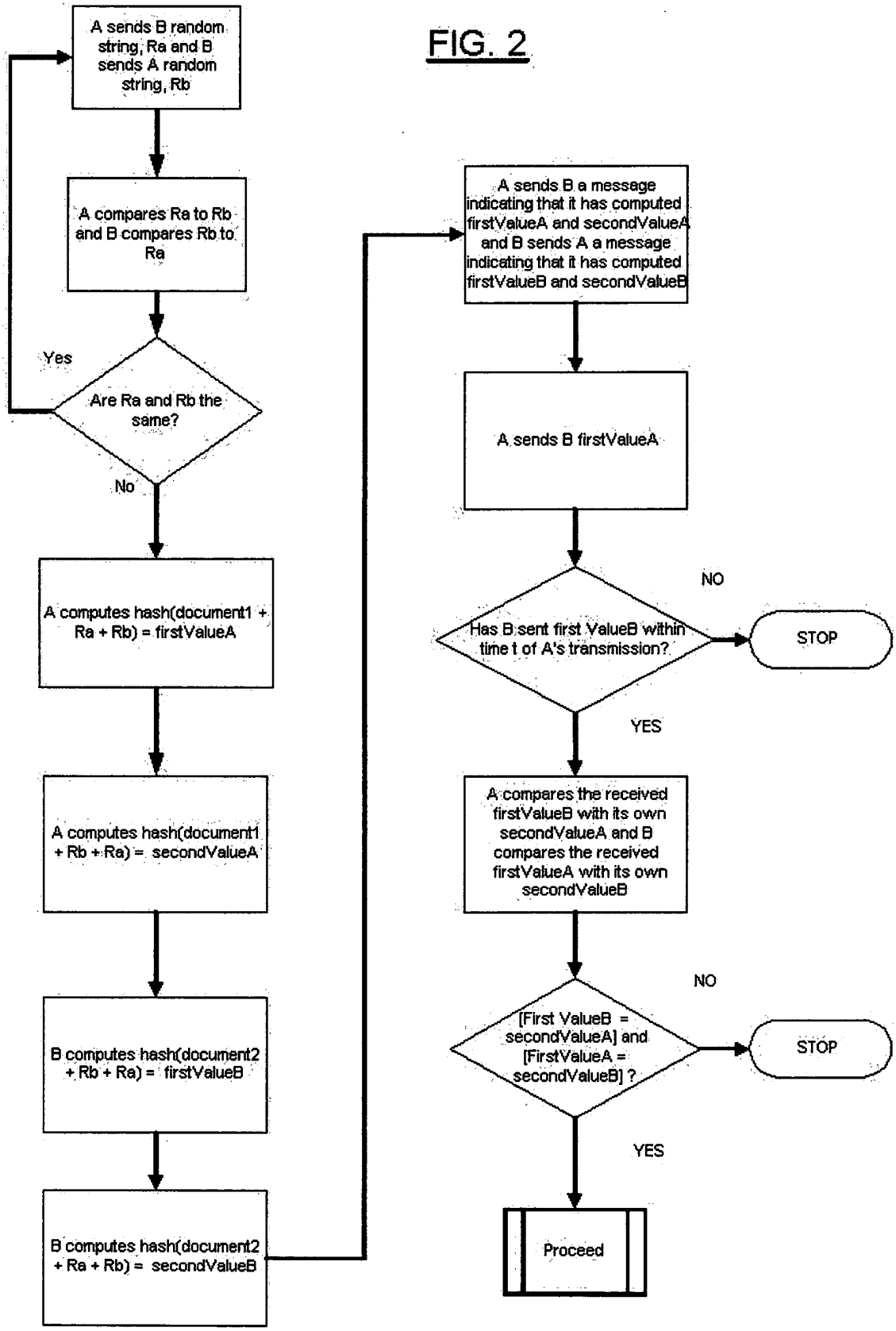


FIG. 1

FIG. 2


A sends B random string, Ra and B sends A random string, Rb
A compares Ra to Rb and B compares Rb to Ra
Yes
Are Ra and Rb the same?
No
A computes hash(document1 + Ra + Rb) = firstValueA
A computes hash(document1 + Rb + Ra) = secondValueA
B computes hash(document2 + Rb + Ra) = firstValueB
B computes hash(document2 + Ra + Rb) = secondValueB
A sends B a message indicating that it has computed firstValueA and secondValueA and B sends A a message indicating that it has computed firstValueB and secondValueB
A sends B firstValueA
NO
Has B sent first ValueB within time t of A's transmission?
STOP
YES
A compares the received firstValueB with its own secondValueA and B compares the received firstValueA with its own secondValueB
NO
[First ValueB = secondValueA] and [FirstValueA = secondValueB] ?
STOP
YES
Proceed